Security Update for Our API Consumers

Effective June 1, 2017, ACS Technologies will disable Transport Layer Security 1.0 and 1.1 (TLS 1.0 and TLS 1.1) across all of our services.

Effects of disabling TLS 1.0 and 1.1

The TLS security protocol encrypts information exchanged between electronic devices over the Internet, and it is updated regularly to keep pace with security weaknesses. Keeping TLS 1.0 and 1.1 enabled would leave your organization and your contributors' online data vulnerable to fraud and identity theft.

If you use our public APIs to develop customized solutions, and they're configured to use TLS 1.0 or TLS 1.1, those APIs will no longer work.

What you need to do

Upgrade to the current industry standard – TLS 1.2:

- Ensure the operating systems and browsers on your hosting servers and PCs are configured to function with TLS 1.2.
- Run this compatibility test on your PCs and hosting servers to verify they're compatible with TLS 1.2. When testing the API's, make sure you navigate to the compatibility test site and activate the API call from the servers that host your custom solutions.
- Inform your congregants and contributors to upgrade their browsers to be compatible with TLS 1.2.

Your security is our highest priority

Upgrading computer systems often requires time and money, and we empathize with your concerns about it. Please realize this is necessary to help maintain the best online security protection for your organization.

We thank you for your continuing partnership and cooperation with us.

If you have any questions, please contact us at 1-800-669-2509.